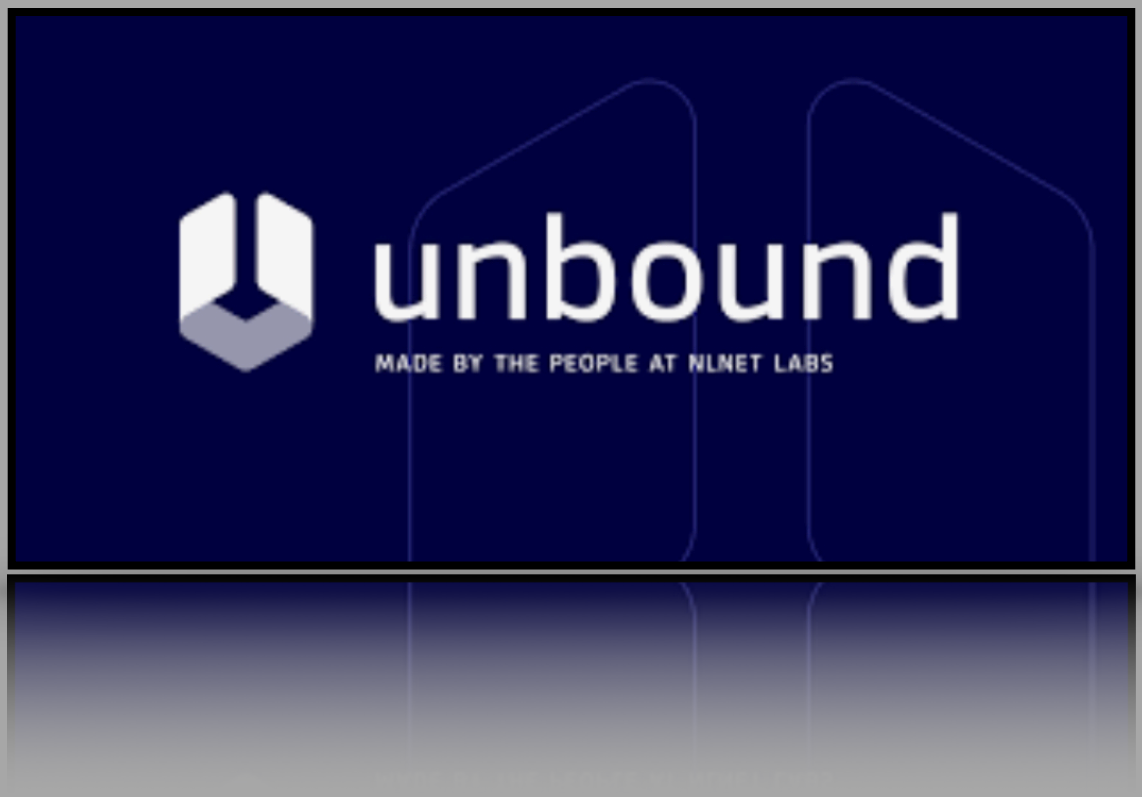
UNBOUND DNS



INSTALL UNBOUND

$ apt install unbound unbound-host -y

$ curl -o /var/lib/unbound/root.hints https://
www.internic.net/domain/named.cache

 # Create Unbound conf file
$ nano /etc/unbound/unbound.conf

 # Copy / Paste config file below.

```
server:
  num-threads: 1

  #Enable logs
  verbosity: 1
```

```
#list of Root DNS Server
root-hints: "/var/lib/unbound/root.hints"

#Respond to DNS requests on all interfaces
interface: 0.0.0.0
max-udp-size: 3072

#Authorized IPs to access the DNS Server
access-control: 0.0.0.0/0               refuse
access-control: 127.0.0.1                allow
access-control: 192.168.20.0/24         allow

#not allowed to be returned for public internet  names
private-address: 192.168.20.0/24

# Hide DNS Server info
hide-identity: yes
hide-version: yes

#Limit DNS Fraud and use DNSSEC
```

```
  harden-glue: yes
  harden-dnssec-stripped: yes
  harden-referral-path: yes

  #Add an unwanted reply threshold to clean the cache and
avoid when possible a DNS Poisoning
  unwanted-reply-threshold: 10000000

  #Have the validator print validation failures to the log.
  val-log-level: 1

  #Minimum lifetime of cache entries in seconds
  cache-min-ttl: 1800

  #Maximum lifetime of cached entries
  cache-max-ttl: 14400
  prefetch: yes
  prefetch-key: yes

# End Config file
```

Systemd

Now you need to ensure that systemd-resolved is not occupying the DNS port. You can do this by giving it the following configuration file:

$ nano /etc/systemd/resolved.conf
[Resolve]
DNS=127.0.0.1
FallbackDNS=1.0.0.1
MulticastDNS=no
DNSStubListener=no

Remove Systemd-resolved

 # Restart systemd-resolved with :

$ systemctl restart systemd-resolved.service

 # Stop systemd-resolved with:

$ systemctl stop systemd-resolved.service

 # Disable systemd-resolved with:

$ systemctl disable systemd-resolved.service

Now enable unbound

 # Then Start and Enable Unbound:

$ systemctl start unbound.service

 # To make it start on every boot:

$ systemctl enable unbound.service

Common Commands

 # Access unbound CLI

$ unbound-control-setup

 # The add this to the config file at bottom

---

remote-control:

```
    # Enable remote control with unbound-control(8) here.
    # set up the keys and certificates with unbound-control-
setup.
    control-enable: yes

    # what interfaces are listened to for remote control.
    # give 0.0.0.0 and ::0 to listen to all interfaces.
    control-interface: 127.0.0.1

    # port number for remote control operations.
    control-port: 8953

    # unbound server key file.
    server-key-file: "/etc/unbound/unbound_server.key"

    # unbound server certificate file.
    server-cert-file: "/etc/unbound/unbound_server.pem"

    # unbound-control key file.
    control-key-file: "/etc/unbound/unbound_control.key"
```

```
    # unbound-control certificate file.
    control-cert-file: "/etc/unbound/unbound_control.pem"
```

```
$ service unbound restart
$ unbound-checkconf
$ unbound-control status
```

Forward Traffic though the Server

```
$ nano  /etc/sysctl.conf
#net.ipv4.ip_forward = 1
$ sysctl -p
```

Unbound firwall rules

ufw allow from 192.168.20.0/24

ufw allow 41194/any

ufw allow 22/tcp

ufw enable

ufw status

 # Test to see if unbound is working

$ nslookup google.com 127.0.0.1

$ nslookup google.com 192.168.20.1